A Comparison of the Proposed Rule and Final Rule for 21 Code of Federal Regulations, Part 11; Electronic Records; Electronic Signatures

Proposed Part 11	Final Part 11
Part 11 - Electronic Records; Electronic Signatures	**Part 11 - Electronic Records; Electronic Signatures**
Subpart A- General Provisions	**Subpart A- General Provisions**
Sec.	**Sec.**
11.1 Scope.	**11.1 Scope.**
11.2 Implementation.	**11.2 Implementation.**
11.3 Definitions.	**11.3 Definitions.**
Subpart B - Electronic Records	**Subpart B - Electronic Records**
11.10 Controls for closed systems.	**11.10 Controls for closed systems.**
11.30 Controls for open systems.	**11.30 Controls for open systems.**
11.50 Signature manifestations.	**11.50 Signature manifestations.**
11.70 Signature/record binding.	**11.70 Signature/record linking.**
Subpart C - Electronic Signatures	**Subpart C - Electronic Signatures**
11.100 General requirements.	**11.100 General requirements.**
11.200 Identification mechanisms and controls.	**11.200 Electronic signature components and controls.**
11.300 Controls for identification codes/passwords.	**11.300 Controls for identification codes/passwords.**
Authority: Secs. 201-902 of the Federal Food, Drug, and Cosmetic Act. 52 Stat. 1040 *et seq.*, as amended (21 U.S.C. 301-392).	**Authority:** Secs. 201-903 of the Federal Food, Drug, and Cosmetic Act;. (21 U.S.C. 321-393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).
--	--
Subpart A--General Provisions	**Subpart A--General Provisions**
§ 11.1 Scope.	**§ 11.1 Scope.**
(a) The regulations in this part set forth the criteria under which the Food and Drug Administration considers electronic records, electronic signatures, and handwritten signatures executed to electronic records, to be trustworthy, reliable, and generally equivalent to paper records and handwritten	(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records, to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

signatures executed on paper.	
(b) These regulations apply to records in electronic form that are created, modified, maintained, or transmitted, pursuant to any records requirements set forth in chapter I of this title.	(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.
(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required throughout this chapter, unless specifically exempted by regulation that is effective on or after the effective date of this part.	(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.
(d) Electronic records that meet the requirements of this part may be used in lieu of paper based records, in accordance with § 11.2, unless paper based records are specifically required.	(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.
(e) Computer systems (including hardware and software), controls, and attendant documentation maintained pursuant to this part shall be readily available for, and subject to, FDA inspection.	(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.
--	--
§ 11.2 Implementation.	**§ 11.2 Implementation.**
(a) For records required by chapter I of this title to be maintained, but not submitted to the agency, persons may use electronic records/signatures in lieu of paper records/conventional signatures, in whole or	(a) For records required to be maintained, but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the

in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records/signatures in lieu of paper records/conventional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts(s) of a document to be submitted has/have been identified in public docket (docket number to be determined) as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic format without paper records and to which specific receiving unit(s) of the agency (e.g., specific center, office, division, branch) such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons should consult with the intended agency receiving unit for details on how and if to proceed with the electronic submission.

--

requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit (s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

--

§ 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-902, 52 Stat. 1040 et seq., as amended (21 U.S.C. 301-392).

(2) Agency means the Food and Drug Administration.

(3) Biometric/behavioral links means a method of verifying a person's identity based on measurement of the person's physical feature(s) or repeatable action(s).

(4) Closed system means an environment in which there is communication among multiple persons, where system access is restricted to people who are part of the organization that operates the system.

(5) Electronic record means a document or writing comprised of any combination of text,

§ 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 301-393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial or other information

graphic representation, data, audio information, or video information, that is created, modified, maintained, or transmitted in digital form by a computer or related system.

representation in digital form, that is created, modified, maintained, archived, retrieved or distributed by a computer system.

(6) Electronic signature means the entry in the form of a magnetic impulse or other form of computer data compilation of any symbol or series of symbols, executed, adopted or authorized by a person to be the legally binding equivalent of the person's handwritten signature.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols, executed, adopted or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(7) Handwritten signature means the name of an individual, handwritten in script by that individual, executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen, or stylus is preserved. However, the scripted name, while conventionally applied to paper, may also be applied to other devices which capture the written name.

(8) *Handwritten signature* means the scripted name or legal mark of an individual, handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(8) Open system means an environment in which there is electronic communication among multiple persons, where system access extends to people who are not part of the organization that operates the system.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B--Electronic Records

§ 11.10 Controls for closed systems.

Closed systems used to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to conclusively discern invalid or altered records.

(b) The ability to generate true copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(e) Use of time stamped audit trails to document record changes, all write to file operations, and to independently record the date and time of operator entries and actions. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as required for the subject electronic documents and shall be available for agency review and copying.

(f) Use of operational checks to enforce

Subpart B--Electronic Records

§ 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

(f) Use of operational system checks to enforce

permitted sequencing of events, as appropriate.

(g) Use of authority checks to ensure that only those individuals who have been so authorized can use the system, electronically sign a record, access the operation or device, alter a record, or perform the operation at hand.

(h) Use of device (e.g., terminal) location checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(i) Confirmation that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(j) The establishment of, and adherence to, written policies which hold individuals accountable and liable for actions initiated under their electronic signatures, so as to deter record and signature falsification.

(k) Use of appropriate systems documentation controls including:

(i) Adequate controls over the distribution, access to, and use of documentation for system operation and maintenance.

(ii) Records revision and change control procedures to maintain an electronic audit trail that documents time-sequenced development and modification of records.

--

§ 11.30 Controls for open systems

Open systems used to create, modify, maintain, or transmit electronic records shall

permitted sequencing of steps and events, as appropriate.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

--

§ 11.30 Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall

employ procedures and controls designed to ensure the authenticity, integrity and confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and such additional measures as document encryption and use of established digital signature standards acceptable to the agency, to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

--

§ 11.50 Signature manifestations

(a) Electronic records which are electronically signed shall display, in clear text, the printed name of the signer and the date and time when the electronic signature was executed.

(b) Electronic records shall clearly indicate the meaning (such as review, approval, responsibility, and authorship) associated with their attendant signatures.

--

§ 11.70 Signature/record binding

Electronic signatures and handwritten signatures executed to electronic records shall be verifiably bound to their respective electronic records to ensure that the

employ procedures and controls designed to ensure the authenticity, integrity and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and such additional measures as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

--

§ 11.50 Signature manifestations

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and,

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

--

§ 11.70 Signature/record linking

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied or

signatures cannot be excised, copied or otherwise transferred so as to falsify another electronic record.

--

Subpart C--Electronic Signatures

§ 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused or reassigned to anyone else.

(b) Before an electronic signature is assigned to a person, the identity of the individual shall be verified by the assigning authority.

(c) Persons utilizing electronic signatures shall certify to the agency that their electronic signature system guarantees the authenticity, validity, and binding of any electronic signature. Persons utilizing electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is authentic, valid, and binding. The certification should be submitted to the agency district office in which territory the electronic signature system is in use.

--

§ 11.200 Identification mechanisms and controls.

otherwise transferred so as to falsify an electronic record by ordinary means.

--

Subpart C--Electronic Signatures

§ 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(b) Before an organization establishes, assigns, certifies or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form, and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC- 100), 5600 Fishers Lane, Rockville, MD 20857.

(2)Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

--

§ 11.200 Electronic signature components and controls.

(a) Electronic signatures which are not based upon biometric/behavioral links shall:

(1) Employ at least two distinct identification mechanisms (such as an identification code and password), each of which is contemporaneously executed at each signing;

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than it's

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two

genuine owner requires collaboration of two or more individuals.	or more individuals.
(b) Electronic signatures based upon biometric/behavioral links shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.
--	--
§ 11.300 Controls for identification codes/passwords.	**§ 11.300 Controls for identification codes/passwords.**
Electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:
(a) Maintaining the uniqueness of each issuance of identification code and password.	(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
(b) Ensuring that identification code/password issuances are periodically checked, recalled, or revised.	(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised, (e.g., to cover such events as password aging).
(c) Following loss management procedures to electronically deauthorize lost tokens, cards, etc., and to issue temporary or permanent replacements using suitable, rigorous controls for substitutes.	(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and detect and report in an emergent manner any attempts at their unauthorized use to the system security unit, and to organizational management.	(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.
(e) Initial and periodic testing of devices, such as tokens or cards, bearing the	(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate

identifying information, for proper function.

identification code or password information, to ensure that they function properly and have not been altered in an unauthorized manner.

March 1997